Claims (clean copy)

1. A method for handling encrypted user data objects (vNDO),

wherein a rights object (RO) is generated for the encrypted user data object (vNDO) by a data provisioning component (D), which rights object (RO) has assignment information (Content ID) for assigning the rights object (RO) to a container object (DCF) having an encrypted user data object (vNDO), decryption information for decryption information for decrypting the encrypted user data object, and rights information for describing the usage rights of the encrypted user data object, and

wherein a confirmation object (DCFV) assigned to the rights object (RO) is generated by the data provisioning component (D), which confirmation object (DCFV) has assignment information for assigning the rights object (RO) to an encrypted user data object and a checksum of the encrypted user data object (vNDO), comprising the following steps:
Transmit a container object (DCF) to a first telecommunications device (A), the container object (DCF) having a content section (IA), in which an encrypted user data object (vNDO) is provided, and a description section (BA), in which a determined checksum of the encrypted user data object (vNDO) is provided;

Extract the checksum from the description section (BA) of the container object (DCF);

Re-determine the checksum of the encrypted user data object (NDO) provided in the content section (IA) of the container object (DCF);

Compare the extracted checksum with the newly determined checksum so that, in the event that the two checksums tally, an error-free transmission of the encrypted user data object (vNDO) can be concluded,

and in addition:

Request on the part of the first telecommunications device (A) for the confirmation object (DCFV) assigned to the rights object (RO) to be transmitted to said device;

Transmit the confirmation object (DCFV) from the data provisioning component (D) to the first telecommunications device (A);

Extract the checksum from the confirmation object (DCFV);

Compare the checksum extracted from the confirmation object with the newly determined checksum so that, in the event that the two checksums tally, compatibility of the rights object assigned to the confirmation object and the encrypted user data object transmitted to the first telecommunications device (A) in the container object (DCF) can be concluded.

2. The method as claimed in claim 1, wherein a data provisioning component (D) provides user data objects (NDO) which are processed according to the following steps:

Encrypt a user data object (NDO) provided on the data provisioning component (D);

Determine a checksum of the encrypted user data object (vNDO);

Generate a container object (DCF) having a content section (IA), in which the encrypted user data object (vNDO) is provided, and a description section (BA), in which the determined checksum of the encrypted user data object (vNDO) is provided;

Transmit the container object (DCF) from the data provisioning component (D) to the first telecommunications device (A).

3. The method as claimed in one of the claims 1 or 2, wherein the container object (DCF) is transmitted to the first telecommunications device (A) by the data provisioning component (D) via at least one further data provisioning component or at least one further telecommunications device.

4. The method as claimed in one of the claims 1 to 3, wherein a request is submitted on the part of the first telecommunications device (A) to transmit the rights object (RO) generated by the data provisioning component (D) to said telecommunications device.

5. The method as claimed in one of the claims 1 to 3, wherein the rights object (RO) is transmitted by the data provisioning component (D) to the first telecommunications device (A), in particular if compatibility has been established on the basis of an agreement of the checksums of the confirmation object assigned to the rights object and the encrypted user data object transmitted to the first telecommunications device in the container object.

6. The method as claimed in one of the claims 1 to 5, wherein the following steps are performed following a successful comparison of the extracted checksum with the newly determined checksum:

Request description information (BI1) relating to the content of the encrypted user data object (vNDO) from a data provisioning component (D);

Transmit the requested description information (BI1) from the data provisioning component (D) to the first telecommunications device (A);

Check whether the content having the attributes specified in the description information (BI1) can be used by the first telecommunications device (A).

7. A method for handling encrypted user data objects (vNDO) comprising the following steps:

Provide an encrypted user data object (vNDO) in a first telecommunications device (A);

Request description information (BI1) relating to the content of the encrypted user data object (vNDO) from a data provisioning component (D);

Transmit the requested description information (BI1) from the data provisioning component (D) to the first telecommunications device (A);

Check whether the content having the attributes specified in the description information (BI1) can be used by the first telecommunications device (A);

Request from the data provisioning component (D) upon successful checking of the attributes specified in the description information (BI1) a confirmation object (DCFV) which is assigned to a rights object (RO) assigned to the encrypted user data object in order to check the compatibility of the rights object and the encrypted user data object (vNDO).

8. The method as claimed in claim 7, wherein the rights object (RO) is transmitted by the data provisioning component (D) to the first telecommunications device (A) upon successful checking of the compatibility of the rights object and the encrypted user data object.

9. The method as claimed in claim 7 or 8, wherein the encrypted user data object is provided in a content section (IA) of a container object (DCF).

10. The method as claimed in claim 9, wherein the container object (DCF) also has a description section (BA) in

which a checksum of the encrypted user data object (vNDO) is provided.

11. The method as claimed in claim 10, wherein the address of the data provisioning component is also provided in the description section (BA) of the container object (DCF) for the purpose of requesting the description information and/or the confirmation object.

12. The method as claimed in claim 10 or 11, wherein the confirmation object has a checksum of the encrypted user data object (vNDO), the compatibility of the rights object and the encrypted user data object being checked by means of the following steps:

Extract the checksum from the confirmation object (DCFV);

Compare the checksum extracted from the confirmation object with the checksum provided in the description section (BA) of the container object (DCF) so that, in the event that the two checksums tally, the compatibility of the rights object assigned to the confirmation object and the encrypted user data object provided in the container object (DCF) transmitted to the first telecommunications device (A) can be concluded.

13. The method as claimed in one of the claims 1 to 12, wherein a first confirmation message is sent by the first telecommunications device (A) to the data provisioning component (D) if the compatibility of the rights object assigned to the confirmation object and

the encrypted user data object (vNDO) transmitted to the first telecommunications device (A) in the container object (DCF) has been established and/or wherein a second confirmation message is sent if the first telecommunications device has received the rights object from the data provisioning component.

14. The method as claimed in claim 4, 5 or 9 to 13, wherein charging information relating to the transmitted rights object (RO) is transmitted to the telecommunications subscriber assigned to the first telecommunications device (A).

15. The method as claimed in one of the claims 1 to 6 or 10 to 14, wherein the checksum is a hash value calculated according to a hash algorithm.

16. The method as claimed in one of the claims 1 to 15, wherein the first and/or the at least second telecommunications device are part of a first telecommunications network, in particular in the embodiment of a mobile radio network.

17. The method as claimed in one of the claims 1 to 16, wherein the data provisioning component is part of a second telecommunications network.

18. The method as claimed in one of the claims 1 to 17, wherein the first and/or second telecommunications device comprise a radio module and are embodied in particular as a mobile phone, a cordless telephone, or a portable computer.

19. The method as claimed in claim 18, wherein the data is transmitted from and to the first and/or second telecommunications device by means of WAP protocols.

20. The method as claimed in one of the claims 1 to 18, wherein the data is transmitted from and to the first and/or second telecommunications device by means of Internet protocols such as the Hypertext Transfer Protocol.

21. The method as claimed in one of the claims 1 to 20, wherein the user data objects contain text information, audio information, video information, executable programs, software modules or a combination of the aforesaid types of information.

22. A telecommunications arrangement comprising a data provisioning system having at least one data provisioning component (D) and at least one first telecommunications device (A), the telecommunications arrangement being designed for performing a method as claimed in one of the claims 1 to 21.

23. A data provisioning component which is designed for performing a method as claimed in one of the claims 1 to 21.

24. A telecommunications device which is designed for performing a method as claimed in one of the claims 1 to 21.